Fourier-Motzkin method for failure diagnosis in petri net models of discrete event systems

Al-Ajeli, Ahmed; Bordbar, Behzad

DOI:
10.1109/WODES.2016.7497843

Document Version
Peer reviewed version

Citation for published version (Harvard):
Al-Ajeli, A & Bordbar, B 2016, Fourier-Motzkin method for failure diagnosis in petri net models of discrete event systems. in *Proceedings of the 13th International Workshop on Discrete Event Systems (WODES 2016).* IEEE Computer Society Press, 13th International Workshop on Discrete Event Systems (WODES 2016), 30/05/16. https://doi.org/10.1109/WODES.2016.7497843

Fourier-Motzkin Method for Failure Diagnosis in Petri Net Models of Discrete Event Systems

Ahmed Al-Ajeli and Behzad Bordbar

***Abstract*— This paper presents a new technique for failure diagnosis in partially observable discrete event systems modelled as Petri nets. In this new technique we adopt Integer Fourier-Motzkin Elimination (IFME) method. We start with a Petri net and produce the *state equations*. The state equations are a set of integer valued inequalities in variables that represent number of firing of transitions. Occurrences of failure can also be expressed by inequalities. Then we extend the set of inequalities obtained from the state equations to two new sets. The first is created from adding the inequality for failure. The second is created from adding the negation of the inequality for failure. Applying the IFME method to the two resulting sets of inequalities, the variables corresponding to unobservable transitions will be eliminated. Then we prove that for *acyclic* Petri nets, the reduced set of inequalities after the elimination can be used to diagnose failures.**

I. Introduction

Research into failure diagnosis in partially observable discrete event systems (DES) has received considerable attention in the past three decades. A popular approach is to assume existence of a formal representation of the plant behaviour captured in a modelling language. Two common modelling languages are often used; Automata and Petri nets [1]–[5]. Using these languages, failures are modelled as unobservable transitions. Among others, the seminal paper by Sampath *et al*. [1] formulates the diagnosis and diagnosability problem in the systems modelled by Automata. Petri nets provide a rich modelling environment and are widely used in model based failure diagnosis [6] and [3]. An overview of the different approaches suggested for failure diagnosis in discrete event systems can be found in [7]. Here, we use Petri nets for modelling of the plant.

In this paper, we introduce a new approach for failure diagnosis in partially observable discrete event systems using Integer Fourier-Motzkin Elimination (IFME) method. Fourier-Motzkin Elimination (FME) is a method to solve a set of inequalities in real variables [8]–[11]. FME method is an extension of Gaussian elimination method which is commonly used in equations. Similar to Gaussian elimination, FME eliminates variables from a set of inequalities obtaining inequalities with fewer variables. IFME method is an extension of the classic FME to cope with integer valued variables [12] and [13].

The outline of the method suggested in this paper is as follows. We start with a Petri net and produce the *state equations*, denoted E, [14]. The state equations are a set of integer valued inequalities in variables that represent number of firing of transitions. Occurrences of failure can also be expressed by inequalities. This can be done as follows. Assume that t_n is a failure transition. Then the inequality of the form $\mathbf{c} := x_n \leq 0$, where x_n is a variable representing the number of firing t_n in a given firing sequence σ, holds if σ does not contain t_n. Clearly, the negation of this inequality expresses the occurrence of the failure. After modelling failure as an inequality of the form $\mathbf{c}' := x_n > 0$, we simultaneously create two sets of inequalities by adding the inequality $\mathbf{c}$ and negation of $\mathbf{c}$ ($\mathbf{c}'$) to E. Then we apply the IFME to the created sets, denoted $E \cup \{\mathbf{c}\}$ and $E \cup \{\mathbf{c}'\}$, by eliminating all variables corresponding to unobservable transitions. Suppose we denote the resulting sets of inequalities as R and R' respectively. Then we prove that for acyclic Petri nets, R and R' can be used to diagnose failure. The advantage of using R and R' is that since all variables relate to observable events, we can check that for a given sequence σ, if the projection to observable events satisfies R and R'.

This paper is organized as follows. Section II presents a brief introduction to Petri nets' theory and FME method. Modelling of failure via inequalities and a formulation of failure diagnosis is described in section III. Section IV describes our main results involving using IFME for failure diagnosis. We end the paper with related works and conclusions.

II. Preliminary

A. Petri nets

In [14] a *Petri net* is defined as a four tuple $\mathcal{N} = (P, T, pre, post)$, where P and T are two nonempty finite sets of places and transitions, respectively. We denote $m = |P|$ and $n = |T|$ as the number of places and transitions. $pre : P \times T \to \mathbb{N}$ and $post : P \times T \to \mathbb{N}$. For a given transition t, an *input* (*output*) place of t is a place p such that $pre(p,t)$ ($post(p,t)$) is positive, respectively. $A = [a_{ij}]$ is an $n \times m$ matrix of integers called *incidence matrix*, where $a_{ij} = post(p,t) - pre(p,t)$ assuming that the set of places are ordered to correspond the coordinates of the matrix. In this paper $\mathbb{N} = \{0, 1, 2, \dots\}$ is the set of non-negative integers, $\mathbb{Z}$ is the set of all integers and $\mathbb{R}$ is the set of real numbers.

A *state* of a Petri net, known as a *marking*, is represented as $M : P \to \mathbb{N}$ capturing the number of tokens in each place. We sometimes represent a marking as an $m \times 1$ matrix of non-negative integers. A transition t is *enabled* at a marking M if for each $M \geq pre(.,t)$, where $pre(.,t)$ is an $n \times 1$ matrix with coordinates $pre(p,t)$ for $p \in P$. An enabled transition

This work was supported by School of Computer Science, University of Birmingham, Birmingham B15 2TT, United Kingdom.

Ahmed Al-Ajeli and Behzad Bordbar are with school of Computer Science, University of Birmingham, United Kingdom {A.K.O.Al-Ajeli, B.Bordbar}@cs.bham.ac.uk

can *fire* resulting in a new marking M', denoted by $M \xrightarrow{t} M'$, where $M' = M + A(.,t)$. A sequence of transitions $\sigma = t_1 \dots t_k$ of T is called *enabled* at a marking M, if there are marking $M_1, \dots, M_k$ so that $M \xrightarrow{t_1} M_1 \xrightarrow{t_2} M_2 \cdots \xrightarrow{t_k} M_k$. In this case, we write $M \xrightarrow{\sigma} M_k$ and refer to M_k as a state *Reachable* from M and σ is the firing sequence. We write $R(\mathcal{N},\ M)$ for the set of all reachable states from M. The initial state of the system is represented by an *initial marking* M_0. We will write $(\mathcal{N},\ M_0)$ for a Petri net with its initial marking M_0.

The set of all finite-length strings of the transitions in T is denoted by T^* and is called the *Kleene-closure* of T. As a result, members of T^* are created from concatenation of finite number of elements of T. In particular, T^* contains the empty string ε, so that $t\varepsilon = \varepsilon t = t$ for all $t \in T$. Every subset of T^* is called a *language on the alphabet* T. Suppose that we have a firing sequence σ of $(\mathcal{N},\ M_0)$, then the *Parikh vector* $\# : T^* \to \mathbb{N}^n$ is a map which assigns to every firing sequence σ a map $\#(\sigma)$ that produces the number of firing each transition in σ. In other words, for $\#(\sigma) : T \to \mathbb{N}$, $\#(\sigma)(t)$ is the number of occurrence of $t \in T$ within the sequence σ. Sometimes, we write $\#(t,\sigma)$ to represent the number of the occurrences of t in σ.

The set of sequences of transitions resulting in a reachable marking is called the *Language* of the Petri net and is denoted by $L(\mathcal{N},\ M_0)$ i.e. $L(\mathcal{N},\ M_0) = \{\sigma \in T^* \mid \exists M\ M_0 \xrightarrow{\sigma} M\}$.

Suppose that a destination marking M is reachable from M_0 in a Petri net $\mathcal{N}$ through a firing sequence σ, we can then find M using the following *state equations*:

$$M = M_0 + A^T \mathbf{x} \geq \vec{\mathbf{0}} \tag{1}$$

where A is the incidence matrix of $\mathcal{N}$, and $\mathbf{x} \in \mathbb{N}^n$ is a n-dimensional column vector with $\mathbf{x} = (x_1, \dots, x_n)$ and $x_i = \#(t_i, \sigma)$ for $t_i \in T$. Then, for any firing sequence σ of $\mathcal{N}$, there exists $\mathbf{x} = \#(\sigma)$ satisfying (1).

Consider the Petri net of Fig. 1, the set of inequalities in (2) represents the state equations for the Petri net.

$$\begin{array}{rrrrrrrrr}
x_1 & & & & & & & \leq & 1 \\
-x_1 & +x_2 & & & & & & \leq & 0 \\
-x_1 & & +x_3 & & & & & \leq & 0 \\
 & -x_2 & & +x_4 & & & -x_7 & \leq & 0 \\
 & & -x_3 & & +x_5 & & +x_7 & \leq & 0 \\
 & & & -x_4 & & +x_6 & & \leq & 0 \\
 & & & & -x_5 & +x_6 & & \leq & 0 \\
-x_1 & & & & & & & \leq & 0 \\
 & -x_2 & & & & & & \leq & 0 \\
 & & -x_3 & & & & & \leq & 0 \\
 & & & -x_4 & & & & \leq & 0 \\
 & & & & -x_5 & & & \leq & 0 \\
 & & & & & -x_6 & & \leq & 0 \\
 & & & & & & -x_7 & \leq & 0
\end{array} \tag{2}$$

Finally, a *directed circuit* in a Petri net is a closed directed path from one node (place or transition) back to itself. A Petri net having no directed circuits is called an *acyclic* Petri net. For this subclass of Petri nets, the state equations in (1) is a necessary and sufficient condition for reachability of markings. For further information about Petri nets, we refer the reader to [14].

B. Fourier-Motzkin Elimination method

Fourier-Motzkin elimination (FME) method has originally been suggested to solve a set of linear inequalities and also to test if the set solvable or not. In other words, given a matrix $A \in \mathbb{R}^{m \times n}$ and a vector $b \in \mathbb{R}^m$, test if a set of inequalities, say E, of the form $A\mathbf{x} \leq \mathbf{b}$, where $\mathbf{x} = (x_1, x_2, \dots, x_n) \in \mathbb{R}^n$ is a vector of variables, has a solution and, if any, find it. As we may multiply each inequality by a positive scalar, we may assume that all entries in the first column of A are 0, +1 or -1. Without lost the generality, the set E can be rewritten as shown in (3). Thus the problem is to solve this set (the inequalities might need to be reordered first).

$$\begin{aligned}
\mathbf{a_i'}\mathbf{x'} \qquad &\leq b_i,\ i = 1, \dots, m_1 \\
\mathbf{a_j'}\mathbf{x'} - x_n &\leq b_j,\ j = m_1 + 1, \dots, m_2 \\
\mathbf{a_k'}\mathbf{x'} + x_n &\leq b_k,\ k = m_2 + 1, \dots, m
\end{aligned} \tag{3}$$

where $\mathbf{x'} = \{x_1, x_2, \dots x_{n-1}\}$, i.e., the same set of variables without x_n. Assume that $l = max(\mathbf{a_j'}\mathbf{x'} - b_j, j = m_1 + 1, \dots, m_2)$ and $u = min(b_k - \mathbf{a_k'}\mathbf{x'}, k = m_2 + 1, \dots, m)$. Since the last two lines of (3) are equivalent to $l \leq x_n \leq u$, then the variable x_n can be eliminated. This yields the *reduced* set R in (4) as an equivalent to the set E in (3):

$$\begin{aligned}
\mathbf{a_i'}\mathbf{x'} &\leq b_i,\ i = 1, \dots, m_1 \\
\mathbf{a_j'}\mathbf{x'} - b_j &\leq b_k - \mathbf{a_k'}\mathbf{x'},\ j = m_1 + 1, \dots, m_2, \\
k &= m_2 + 1, \dots, m
\end{aligned} \tag{4}$$

By repeating this process, we can successively eliminate the last $n-1$ variables $x_n, x_{n-1}, \dots, x_2$, and end up with a set of inequalities in one variable x_1 which is trivial.

Theorem 1. *[11] Assume that the variables $x_{k+1}, \dots, x_n$ have been eliminated in order by using FME method described above from a set of linear inequalities E. This results in the reduced set R. Then $\alpha_1, \dots, \alpha_k$ is a solution of R iff there exists values $\alpha_{k+1}, \dots, \alpha_n$ such that $\alpha_1, \dots, \alpha_k, \alpha_{k+1}, \dots, \alpha_n$ is a solution of E.*

In fact, the FME method described above is appropriate for eliminating the real variables. In case where the variables are integers ($\in \mathbb{Z}$) there is an extension of FME method. This extension is called Integer Fourier-Motzkin Elimination (IFME) method, see [12] and [13]. In this paper, we have chosen the method presented in [13]. This method better meets our needs as it is somewhat simpler and more efficient.

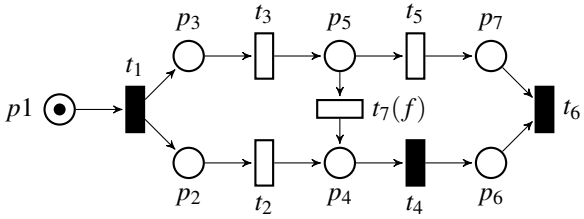

Fig. 1. Example of an *acyclic* Petri net.

For sake of brevity, we have not included the details of IFME method here and for more details we refer the reader to [13].

III. Problem description

In this section we describe the problem of failure diagnosis in DES modelled by Petri nets as outlined in references [15] and [3]. Consider a Petri net $(\mathcal{N},\ M_0)$ with a set of transitions $T = \{t_1, t_2, \ldots, t_n\}$. Suppose that T is partitioned into two sets: observable transitions T_o and unobservable transitions T_u. We further assume that failures are unobservable transitions, i.e., $T_f \subseteq T_u$, in which T_f is the set of transitions which are modelling occurrences of failures. The set T_u may have other transitions which model no failure, i.e., they model normal events. In this paper, we assume that the system has a single failure.

In Petri nets modelling partially observable DES, each observable transition is associated to an event (given as a label). We assume that if a transition fires, the associated event is observed. In other words, in every execution of events, a sequence of transitions from T_o can only be observed. We also assume that there are no two transitions of the Petri nets sharing the same event (label). A Diagnoser (defined below) uses such information to identify if the failure has (not) happened or may have happened.

Also, consider the *projection* function $\pi : T \to T_o \cup \{\varepsilon\}$ that maps unobservable transitions to the empty string ε, i.e. $\pi(t) = \varepsilon$ for $t \in T_u$ while, $\pi(t) = t$ for $t \in T_o$. The projection function π can be extended to the Kleene-closure of T by $\pi : T^* \to (T_o \cup \{\varepsilon\})^*$ where for each sequence of transitions σ and each transition t, $\pi(\sigma t) = \pi(\sigma)\pi(t)$. We assume $\pi(\varepsilon) = \varepsilon$ and that $\pi(t\varepsilon) = \pi(\varepsilon t) = \varepsilon$ for each $t \in T_u$. Likewise, we can define another projection that maps observable transitions for a given sequence to the empty string as $\pi_u : T^* \to (T_u \cup \{\varepsilon\})^*$.

Denote by $\mathbf{s} = \pi(\sigma)$ the observed sequence corresponding to a given firing sequence $\sigma \in T^*$.

Now, based on the definition of the *valuation* described in [16], we shall present the following definition.

Definition 1. *Let $\mathbf{x} = (x_1, \ldots, x_n)$ be a set of variables. We suppose that the variables range over $\mathbb{N}$. A valuation ν for $\mathbf{x}$ is a function that associates a value in $\mathbb{N}$ to each variable x_i in $\mathbf{x}$.*

Remark: In the light of Definition 1, given a sequence $\sigma \in T^*$, Parikh vector $\#(\sigma)$ represents a valuation of $\mathbf{x}$. In other words, for each x_i of $\mathbf{x}$, $x_i = \#(t_i, \sigma)$, where $i = 1, 2, \ldots, n$.

Definition 2. *Suppose that $\mathbf{e}$ is an inequality of the form $a_1x_1 + \cdots + a_nx_n \leq b$ in the variables set $\mathbf{x} = (x_1, \ldots, x_n), x_i \in \mathbb{N}$ and $a_1, \ldots, a_n, b \in \mathbb{N}$. Consider a valuation ν as $\alpha_1, \ldots, \alpha_n$ assigned to value $x_1, \ldots, x_n$ respectively. Then we write $\nu \vDash \mathbf{e}$ to say that the valuation ν satisfies the inequality $\mathbf{e}$ if and only if $a_1\alpha_1 + \cdots + a_n\alpha_n \leq b$.*

Definition 3. *Suppose that we have a set of inequalities $E = \{e_i \mid 1 \leq i \leq d\}$ where e_i has the form of $\mathbf{e}$ in Definition 2. Consider a valuation ν for the variables of the inequalities in E. Then $\nu \vDash E$ iff $\nu \vDash e_1 \wedge \cdots \wedge e_d$ ("$\wedge$" is the conjunctive operator).*

Lemma 1. *Given a Petri net $(\mathcal{N}, M_0)$, we can derive a corresponding set of inequalities E in the form $-A^T\mathbf{x} \leq M_0$ (derived from (1)), where $\mathbf{x} \geq \mathbf{0}$ and A is the incidence matrix of $\mathcal{N}$. If $\mathcal{N}$ is acyclic, then marking M is reachable from M_0, i.e., $M_0 \xrightarrow{\sigma} M$ iff there exists $\mathbf{x}$ satisfying E and $\mathbf{x} = \#(\sigma)$.*

Proof: See the proof of Theorem 16 in [14]. □

In this paper, we use inequalities in two ways. Firstly, the *state equations* constraints can be written as a set of inequalities E. Secondly, failure can also be written as an inequality.

Representation of a failure as an inequality: Suppose that transition $t_i \in T$ is a failure transition. Occurrence of t_i in a firing sequence σ can be trivially written as

$$\#(t_i, \sigma) > 0. \tag{5}$$

On the other hand, we can express the case where t_i does not appear in σ as

$$\#(t_i, \sigma) \leq 0. \tag{6}$$

Now if we consider that the case where there is no t_i in σ corresponds to a satisfaction of a constraint. Likewise, we can say that appearance of t_i in σ corresponds to a violation of the constraint. Let us denote the constraint by $\mathbf{c}$ and the violation of the constraint by $\mathbf{c}'$, i.e., $\mathbf{c}$ and $\mathbf{c}'$ represent the inequalities in (6) and (5) respectively.

In what follows, we shall present the definition of the Diagnoser. This definition is inspired by previous works of [1] and [3].

Definition 4. *A Diagnoser is a function $\Delta : T_o^* \to \{N, F, FN\}$ that associates to each observed sequence $\mathbf{s}$ with respect to the failure modelled by a transition $t \in T_u$ one of the following diagnosis states:*

- *$\Delta(\mathbf{s}) = N$ if $\forall \sigma \in L(\mathcal{N}, M_0)$ and $\pi(\sigma) = \mathbf{s}$, $\#(\sigma) \vDash \mathbf{c}$. This state is NoFault as there is no firing sequence having the same observation containing the failure transition, i.e., no failure has happened.*
- *$\Delta(\mathbf{s}) = F$ if $\forall \sigma \in L(\mathcal{N}, M_0)$ and $\pi(\sigma) = \mathbf{s}$, $\#(\sigma) \vDash \mathbf{c}'$. This state is Faulty as all firing sequences having the same observation containing the failure transition, i.e., the failure has certainly happened during the observed sequence $\mathbf{s}$.*
- *$\Delta(\mathbf{s}) = FN$ if there are two sequences $\sigma_1,\ \sigma_2 \in L(\mathcal{N}, M_0)$, $\pi(\sigma_1) = \mathbf{s}$, $\pi(\sigma_2) = \mathbf{s}$, $\#(\sigma_1) \vDash \mathbf{c}$ and $\#(\sigma_2) \vDash \mathbf{c}'$. In which case, the behaviour of the system is ambiguous because both NoFault and Faulty states are possible during the observed sequence. For this reason, this state is called Uncertain state.*

Example 1: To explain the failures diagnosis notions in Petri nets mentioned above, let us consider the Petri net depicted in Fig. 1. Assume that the initial marking of this net is $M_0 = [1000000]$. The observable transitions are shown by solid rectangles, while empty rectangles represent

unobservable transitions. In this net, there is only one failure modelled by the transition t_7. In this example, the constraint $\mathbf{c}$ can be written as $x_7 \leq 0$ and its negation $\mathbf{c}'$ as $x_7 > 0$.

Assume that no firing of any transition has been observed at the initial marking. In which case, we are certain that no failure has happened as there is no any unobservable transition enabled at the initial marking. Let us also assume that the sequence $\mathbf{s} = t_1$ is observed at the initial marking M_0. By observing this sequence, we are not certain about the diagnosis state as there are at least two possible sequences, for example, $\sigma_1 = t_1t_2$ and $\sigma_2 = t_1t_3t_7$ such that $\sigma_1, \sigma_2 \in L(\mathcal{N}, M_0)$, $\#(\sigma_1) \vDash \mathbf{c}$ and $\#(\sigma_2) \vDash \mathbf{c}'$. Hence, we say that the diagnosis state is *Uncertain*. Likewise, we have the same diagnosis state when the sequence t_1t_4 is observed. In this case we have at least two sequences, for instance $\sigma_1 = t_1t_2t_4$ and $\sigma_2 = t_1t_3t_7t_4$, with $\pi(\sigma_1) = \pi(\sigma_2) = t_1t_4$ such that $\#(\sigma_1) \vDash \mathbf{c}$ but $\#(\sigma_2) \vDash \mathbf{c}'$. In both cases, the failure may have happened, but also the diagnosis state could be *NoFault*. Thus $\Delta(\mathbf{s}) = FN$.

Now suppose that the sequence $\mathbf{s} = t_1t_4t_4$ is observed. In which case, for any $\sigma \in L(\mathcal{N}, M_0)$ such that $\pi(\sigma) = \mathbf{s}$, σ has the transition t_7. As a result, we are certain that $\mathbf{c}$ is violated and the diagnosis state is $\Delta(\mathbf{s}) = F$. On the other hand, observing $\mathbf{s} = t_1t_4t_6$ excludes the possibility of firing any sequence having the transition t_7 as t_6, if fired, requires at least one token in both places p_6 and p_7 and this is impossible in a case where t_7 fires. Hence $\#(\mathbf{s}) \vDash \mathbf{c}$ for all σ such that $\sigma \in L(\mathcal{N}, M_0)$ and $\pi(\sigma) = \mathbf{s}$, i.e., the failure has not occurred during observing the sequence and the diagnosis state is $\Delta(\mathbf{s}) = N$.

IV. Failure diagnosis: main results

In this section, we shall present the main results of our work. Suppose that $\mathcal{N}$ is an *acyclic* Petri net. Without any loss of generality, suppose that we have renamed the transitions of $\mathcal{N}$ such that the first k transitions are observable, i.e., $T_o = \{t_1, t_2, \ldots, t_k\}$. The remaining transitions are unobservable, i.e., $T_u = \{t_{k+1}, t_{k+2}, \ldots, t_n\}$. We further assume that the system has a single failure and t_n is the only failure transition of the system. We introduce variables $x_1, x_2, \ldots, x_n$ representing the number of firing of $t_1, t_2, \ldots, t_n$ as described in section III. Suppose that $E := M_0 + A^T\mathbf{x} \geq \vec{\mathbf{0}}$ represents the state equations, where $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ as explained in section II-A. We further assume that $\mathbf{c}$ is the inequality $x_n \leq 0$ and $\mathbf{c}'$ is the negation of $\mathbf{c}$, i.e., the inequality $x_n > 0$. Apparently, for each firing sequence σ of $(\mathcal{N}, M_0)$, if σ contains t_n, i.e., the failure transition, then $\#(\sigma)$, the Parikh vector of σ, satisfies $\mathbf{c}'$. Conversely, for a firing sequence σ, if $\#(\sigma)$ satisfies $\mathbf{c}$, then σ has no the failure transition t_n.

Fig. 2 depicts a general sketch of our method. Assume that we start with an *acyclic* Petri net model. First, we obtain a set of inequalities $E := M_0 + A^T\mathbf{x} \geq \vec{\mathbf{0}}$. Then, we create two sets of inequalities $E \cup \{\mathbf{c}\}$ and $E \cup \{\mathbf{c}'\}$. Applying IFME method simultaneously to both $E \cup \{\mathbf{c}\}$ and $E \cup \{\mathbf{c}'\}$, we obtain two reduced sets R and R' by eliminating every variable corresponding to a transition in the set T_u. We use

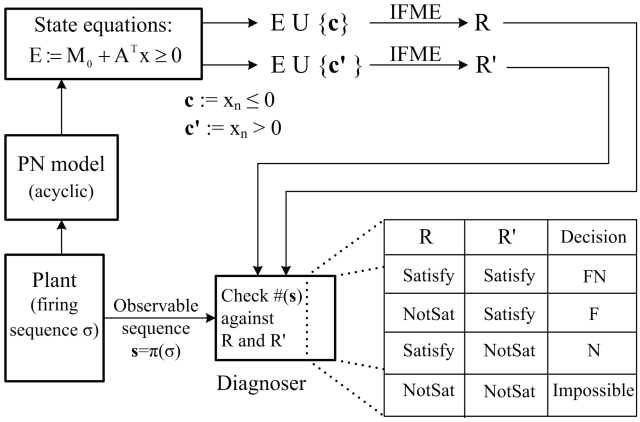

Fig. 2. Sketch of the solution.

the reduced sets of inequalities to diagnose failure occurrence of t_n as follows.

Theorem 2. *Suppose that $\mathcal{N}$ is an acyclic Petri net with an initial marking M_0. Suppose that E is the set of inequalities $-A^T\mathbf{x} \leq M_0$ created from the state equation of $\mathcal{N}$, see Lemma 1. Assume that $T = T_o \cup T_u$, $T_o = \{t_1, \ldots, t_k\}$, $T_u = \{t_{k+1}, \ldots, t_n\}$ and t_n is a failure transition. The vector of variables $x_1, \ldots, x_n$ corresponds to the number of firing the transitions $t_1, \ldots, t_n$. Assume also that $\mathbf{c}$ is the inequality $x_n \leq 0$ and $\mathbf{c}'$ is its negation. Suppose that the set of inequalities R and R' are respectively produced from applying of IFME to both $E \cup \{\mathbf{c}\}$ and $E \cup \{\mathbf{c}'\}$ to eliminate all variables corresponding to transitions in T_u. Then, for any given sequence of observable events $\mathbf{s} = \pi(\sigma)$, where σ is a firing sequence in $\mathcal{N}$ ($M_0 \xrightarrow{\sigma} M$), if*

1) *$\#(\mathbf{s}) \nvDash R$, then $\Delta(\mathbf{s}) = F$ (Faulty).*
2) *$\#(\mathbf{s}) \nvDash R'$, then $\Delta(\mathbf{s}) = N$ (NoFault).*
3) *$\#(\mathbf{s}) \vDash R$ and $\#(\mathbf{s}) \vDash R'$, then $\Delta(\mathbf{s}) = FN$ (Uncertain).*
4) *$\#(\mathbf{s}) \nvDash R$ and $\#(\mathbf{s}) \nvDash R'$, it is not possible to have this case.*

Proof: In what follows assume that $\#(\mathbf{s}) = (\alpha_1, \ldots, \alpha_k)$.

Proof of 1: Assume that $\#(\mathbf{s}) \nvDash R$, but the diagnosis state is not *Faulty*. If $\#(\mathbf{s}) \nvDash R$, then for every valuation $(\alpha_{k+1}, \ldots, \alpha_n)$ of $(x_{k+1}, \ldots, x_n)$ such that $\nu = (\alpha_1, \ldots, \alpha_k, \alpha_{k+1}, \ldots, \alpha_n)$, $\nu \nvDash E \wedge \mathbf{c}$ by Theorem 1. As a result, $\forall \sigma' \in L(\mathcal{N}, M_0)$ such that $\pi(\sigma') = \mathbf{s}$, $\#(\sigma') \vDash \mathbf{c}'$, i.e., $\#(t_n, \sigma') > 0$. Hence the failure has happened during observing $\mathbf{s}$. This contrasts the assumption.

Proof of 2: Using the same argument in **Proof of 1** replacing R with R'.

Note that the proofs of 1 and 2 are still valid for Petri nets which are not *acyclic*.

Proof of 3: Assume that $\#(\mathbf{s}) \vDash R$ and $\#(\mathbf{s}) \vDash R'$, but we are certain about the diagnosis state. If $\#(\mathbf{s}) \vDash R$, then there exists a valuation $(\alpha_{k+1}, \ldots, \alpha_n)$ of $(x_{k+1}, \ldots, x_n)$ such that $\nu = (\alpha_1, \ldots, \alpha_k, \alpha_{k+1}, \ldots, \alpha_n)$ and $\nu \vDash E \wedge \mathbf{c}$ by Theorem 1. If $\nu \vDash E \wedge \mathbf{c}$, then $\nu \vDash E$. Considering that $\mathcal{N}$ is *acyclic*, then there exists σ' such that $M_0 \xrightarrow{\sigma'} M'$, $\#(\sigma') = \nu$. Hence, $\#(t_n, \sigma') \leq 0$ which implies that σ' contains no failure. Now, we claim that $\pi(\sigma') = \mathbf{s}$. The proof of this claim is accomplished by induction on the length of the observed

sequence denoted $|\mathbf{s}|$.
(*Basis step*): If $|\mathbf{s}| = 1$, then $\pi(\sigma') = \mathbf{s}$ because $\#(\pi(\sigma')) = \#(\mathbf{s})$.
(*Induction step*): We assume that the claim is true for all $\mathbf{s}$ with $|\mathbf{s}| \leq k_1$ (*Induction hypothesis*). Also, we prove it true for $\mathbf{s}$ with $|\mathbf{s}| = k_1 + 1$. Suppose $\mathbf{s} = \omega t$ where $t \in T_o$ and $\omega \in T_o^*$. Since $\sigma, \sigma' \in L(\mathcal{N}, M_0)$ and $\#(\pi(\sigma)) = \#(\pi(\sigma')) = \#(\mathbf{s})$, then for $\sigma' = \sigma'_1 t' \sigma'_2$ we have

$M_0 \xrightarrow{\sigma'_1} M'_1 \xrightarrow{t'} M'_2 \xrightarrow{\sigma'_2} M'$, $t' \in T_o$, and $\sigma'_1 \in T^*, \sigma'_2 \in T_u^*$

where t' is the last observable transition of σ'. Also σ'_2 can be empty. For $\sigma = \sigma_1 t \sigma_2$ we have

$M_0 \xrightarrow{\sigma_1} M_1 \xrightarrow{t} M_2 \xrightarrow{\sigma_2} M$, $\sigma_1 \in T^*, \sigma_2 \in T_u^*$

Because $\pi(\sigma) = \mathbf{s} = \omega t$ and t is the last observable transition in σ, then $\pi(\sigma_1) = \omega$. By induction hypothesis, $\pi(\sigma'_1) = \omega$. Since $\#(\pi(\sigma')) = \#(\mathbf{s}) = \#(\omega t)$, then $t = t'$ (if $t \neq t'$ then $\#(\pi(\sigma')) \neq \#(\mathbf{s})$ and this is not true). As a result, $\pi(\sigma') = \pi(\sigma'_1)t' = \omega t = \mathbf{s}$ and this proves the claim.

Similarly, we can prove that if $\#(\mathbf{s}) \vDash R'$, there exists a sequence σ'' such that $M_0 \xrightarrow{\sigma''} M''$, $\#(\sigma'') \vDash \mathbf{c}'$ ($\#(t_n, \sigma'') > 0$) and $\pi(\sigma'') = \mathbf{s}$.

To conclude, since $\sigma', \sigma'' \in L(\mathcal{N}, M_0)$ with $\pi(\sigma') = \pi(\sigma'') = \mathbf{s}$, $\#(\sigma') \vDash \mathbf{c}$ and $\#(\sigma'') \vDash \mathbf{c}'$, hence we have *Uncertain* state, see Definition 4. This contrasts the assumption.

Proof of 4: Assume that $\#(\mathbf{s}) \nvDash R$ and $\#(\mathbf{s}) \nvDash R'$, but this case is possible. If $\#(\mathbf{s}) \nvDash R$, then for every valuation $(\alpha_{k+1}, \ldots, \alpha_n)$ of $(x_{k+1}, \ldots, x_n)$ such that $\nu = (\alpha_1, \ldots, \alpha_k, \alpha_{k+1}, \ldots, \alpha_n)$, $\nu \nvDash E \wedge \mathbf{c}$ by Theorem 1. Also, if $\#(\mathbf{s}) \nvDash R'$, then for every valuation $(\beta_{k+1}, \ldots, \beta_n)$ of $(x_{k+1}, \ldots, x_n)$ such that $\nu = (\alpha_1, \ldots, \alpha_k, \beta_{k+1}, \ldots, \beta_n)$, $\nu \nvDash E \wedge \mathbf{c}'$ by Theorem 1. Rephrasing this statement, we can say that there exists at least one valuation $(\beta_{k+1}, \ldots, \beta_n)$ of $(x_{k+1}, \ldots, x_n)$ such that $\nu = (\alpha_1, \ldots, \alpha_k, \beta_{k+1}, \ldots, \beta_n)$ and $\nu \vDash E \wedge \mathbf{c}$ taking into account that $\mathbf{c}'$ is the violation of $\mathbf{c}$ and σ is a firing sequence of $\mathcal{N}$, i.e., $\#(\sigma) \vDash E$. Here we have contradictory statements. Hence this case is an impossible case. This contrasts the assumption and completes the proof. □

Simply, the above theorem states that given an observed sequence, the satisfaction of the Parikh vector of the sequence is checked against both sets R and R'. Then diagnosis states are estimated according to the outcomes. In particular, if the observable sequence does not satisfy R, then the diagnosis state is *Faulty*. In contrast, if the observable sequence does not satisfy R', then the diagnosis state is *NoFault*. Otherwise, the diagnosis state is *Uncertain*. Note that the case where the observable sequence does not satisfy both R and R' is not possible. Apparently, Theorem 2 provides a systematic procedure to detect firing of the failure transition.

Example 2: Recall that the Petri net of Fig. 1, where the transition failure is t_7, and its associated set of inequalities is as described in (2). Assume that we have augmented this set once by adding the constraint $\mathbf{c} := x_7 \leq 0$ and another by adding the negation of the constraint $\mathbf{c}' := -x_7 \leq -1$ (Note that this inequality is rewritten in the standard form of the set of inequalities defined in Lemma 1, and also the non-negative constraint $x_7 \geq 0$ is previously removed from E). Then, applying IFME method to each augmented set results in the two reduced sets R and R' described in (7) and (8) respectively. Note that all variables corresponding to unobservable transitions $T_u = \{t_2, t_3, t_5, t_7\}$ have been eliminated in both sets. The set of inequalities in (7) and (8) are in variables representing the observable transitions $T_o = \{t_1, t_4, t_6\}$.

$$
\begin{array}{rrrcr}
x_1 & & & \leq & 1 \\
-x_1 & +x_4 & & \leq & 0 \\
-2x_1 & +x_4 & & \leq & 0 \\
 & -x_4 & +x_6 & \leq & 0 \\
-x_1 & & +x_6 & \leq & 0 \\
-2x_1 & +x_4 & +x_6 & \leq & 0 \\
-x_1 & & & \leq & 0 \\
 & -x_4 & & \leq & 0 \\
 & & -x_6 & \leq & 0
\end{array}
\tag{7}
$$

$$
\begin{array}{rrrcr}
x_1 & & & \leq & 1 \\
-x_1 & & +x_6 & \leq & -1 \\
-2x_1 & +x_4 & +x_6 & \leq & 0 \\
 & -x_4 & +x_6 & \leq & 0 \\
-2x_1 & +x_4 & & \leq & 0 \\
-x_1 & & & \leq & -1 \\
 & -x_4 & & \leq & 0 \\
 & & -x_6 & \leq & 0
\end{array}
\tag{8}
$$

Considering these two sets, let the observed sequence $\mathbf{s} = \varepsilon$, then $\#(t_1, \mathbf{s}) = 0$, $\#(t_4, \mathbf{s}) = 0$, $\#(t_6, \mathbf{s}) = 0$ as we have not observed any transition from the set $T_o = \{t_1, t_4, t_6\}$. By looking at (7) and (8), we find that the latter is not satisfied. In which case, we are certain that no failure has happened. Likewise, when $\mathbf{s} = t_1 t_4 t_6$, we have $\#(t_1, \mathbf{s}) = 1$, $\#(t_4, \mathbf{s}) = 1$, $\#(t_6, \mathbf{s}) = 1$. Substituting these values of variables in (7) and (8) establishes that (8) is not satisfied. Thus we conclude a similar diagnosis state, i.e., $\Delta(\mathbf{s}) = N$.

Now, assume that $\mathbf{s} = t_1 t_4 t_4$, then $\#(t_1, \mathbf{s}) = 1$, $\#(t_4, \mathbf{s}) = 2$, $\#(t_6, \mathbf{s}) = 0$. In such a case, (7) is not satisfied which implies that the failure has certainty happened, i.e., we have $\Delta(\mathbf{s}) = F$. Finally, let $\mathbf{s} = t_1 t_4$, this yields $\#(t_1, \mathbf{s}) = 1$, $\#(t_4, \mathbf{s}) = 1$, $\#(t_6, \mathbf{s}) = 0$. Verifying these values against (7) and (8), we obtain that both of them are satisfied. Based on these results, we infer that the failure may have happened, i.e., $\Delta(\mathbf{s}) = FN$.

V. Related work

Failure diagnosis problem in partially observable discrete event systems have first been studied in the Automata framework (see [1]) as mentioned before. That work takes into account the possibility of multiple failures. The notion of solution suggested starts by creating from the model of the system an Automaton called Diagnoser. The Diagnoser is built using the observable events. In fact, the notion adopted uses strings matching method in order to diagnose failures. In other words, using a string of observable events to first find an exact match in the Diagnoser. Then, checking the Diagnoser state reached from the initial state by tracking events in the Diagnoser matching that string.

The results obtained in [1] have been extended in Petri nets setting (see [15]). In that work, the Diagnoser is created using two steps. First, transforming a Petri net into Automaton via building the *reachability graph*. Second, producing the Diagnoser from this Automaton. An improvement to that work has been suggested in [3] through presenting the notion of *basis marking and justifications*.

Obviously, both notions described above employ Automata to represent the Diagnoser. In the work presented in this paper, the Diagnoser has been represented by two sets of inequalities, R and R'. All variables in these two sets represent the number of firing observable transitions. These two sets are first derived from the *state equations* in Petri nets following by application of IFME method. Then observing a sequence of the events, the Diagnoser makes the decisions based on checking the satisfaction of the number of firing transitions in the sequence against R and R'.

As a matter of fact, we are not the first people who work on the equations to diagnose failures in discrete event systems. The state equations usage has been presented in [17] and [5]. In these works, reduction of the failure diagnosis problem to Integer Linear Programming (ILP) problem has been described. Then, a ILP problem has to be solved every time an event is observed. Apparently, the works just mentioned are different from our work as we do not reduce failure diagnosis problem into ILP problem.

With respect to extension of the current work, we summarise the future plan as follows. In fact, we have focused in this paper on diagnosis of a single failure. Imagine that the system has more than one failure transition. The extension of the current work to tackle such a problem can be accomplished as follows. We could produce separated pair of sets of inequalities R_i and R'_i for each failure type i. During the process of production, all other transitions belonging to the other failure types are considered as other unobservable transitions.

In addition, the assumptions made in this paper can be relaxed. In particular, regarding the cyclicity assumption, we can include wider subclasses of Petri nets having cycles, namely *trap* and *siphon circuit* Petri nets. In these subclasses a necessary and sufficient condition for reachability is available (see [18]). Simultaneously, relaxation of the assumption where two different transitions are not permitted to have same labels could be a part of the following work.

Finally, another future direction of research is the *diagnosability*, i.e., the property of the system in which any failure occurrence can be diagnosed after a finite delay. The problem of diagnosability has been presented in Automata setting and then extended in Petri nets framework. Our goal is to study this problem in the context of suggested approach.

VI. Conclusions

In this paper, a new approach is introduced to address failures diagnosis problem in discrete event systems modelled by *acyclic* Petri nets. The systems under study are partially observable where failures are modelled as unobservable transitions. In this new approach, we introduce a different technique to produce the Diagnoser. In fact, the Diagnoser here is no longer represented as an Automaton but as a pair of sets of inequalities in variables representing the number of firing observable transitions. To produce these sets, IFME method is applied. This method eliminates the variables representing unobservable transitions from a set of inequalities representing *state equations* in Petri nets. Previously, we create two sets after adding the constraint (normal behaviour) and its negation (faulty behaviour) to state equations. The two resulting sets are used for diagnosis purposes. The suggested approach has been applied to systems with a single failure. The extension to include systems with multiple failures seems to be straightforward. In parallel, we can relax the cyclicity assumption somewhat. Overall, we hope that this approach opens a new direction for research in the field of the failure diagnosis.

References

[1] M. Sampath, R. Sengupta, S. Lafortune, K. Sinnamohideen, and D. Teneketzis, "Diagnosability of discrete-event systems," *IEEE Transactions on Automatic Control*, vol. 40, no. 9, pp. 1555–1575, 1995.

[2] S. Genc and S. Lafortune, "Distributed diagnosis of Place-Bordered Petri nets," *IEEE Transactions on Automatic Science and Enginnering*, vol. 4, no. 2, pp. 206–219, 2007.

[3] M. P. Cabasino, A. Giua, and C. Seatzu, "Fault detection for discrete event systems using petri nets with unobservable transitions," *Automatica*, vol. 46, no. 9, pp. 1531–1539, 2010.

[4] F. Basile, P. Chiacchio, and G. D. Tommasi, "Sufficient conditions for diagnosability of Petri nets," in *Proceedings of the 9th International Workshop on Discrete Event Systems*, Göteborg, Sweden, May 2008.

[5] M. Dotoli, M. P. Fanti, A. M. Mangini, and W. Ukovich, "On-line fault detection of discrete event systems by Petri nets and integer linear programming," *Automatica*, vol. 45, no. 11, pp. 2665–2672, 2009.

[6] G. Jiroveanu, R. K. Boel, and B. Bordbar, "On-line monitoring of large Petri net models under partial observation," *Discrete Event Dynamic Systems*, vol. 18, pp. 323–354, 2008.

[7] J. Zaytoon and S. Lafortune, "Overview of fault diagnosis methods for discret event systems," *Annual Review in Control*, vol. 37, pp. 308–320, 2013.

[8] H. W. Kuhn, "Solvability and consistency for linear equations and inequalities," *The American Mathematical Monthly*, vol. 63, no. 4, pp. 217–232, 1956.

[9] D. A. Kohler, "Projections of convex polyhedral sets." DTIC Document, Tech. Rep., 1967.

[10] G. B. Dantzig, "Fourier-motzkin elimination and its dual," DTIC Document, Tech. Rep., 1972.

[11] R. Duffin, "On fourier's analysis of linear inequality systems," in *Pivoting and Extension*, ser. Mathematical Programming Studies, M. Balinski, Ed. Springer Berlin Heidelberg, 1974, vol. 1, pp. 71–95. [Online]. Available: http://dx.doi.org/10.1007/BFb0121242

[12] H. P. Williams, "Fourier-motzkin elimination extension to integer programming problems," *Journal of Combinatorial Theory, Series A*, vol. 21, no. 1, pp. 118–123, 1976.

[13] W. Pugh, "The omega test: a fast and practical integer programming algorithm for dependence analysis," in *Proceedings of the 1991 ACM/IEEE conference on Supercomputing*. ACM, 1991, pp. 4–13.

[14] T. Murata, "Petri nets: Properties, analysis and applications," *Proceedings of the IEEE*, vol. 77, no. 4, pp. 541–580, April 1989.

[15] S. Genc and S. Lafortune, "Distributed diagnosis of discrete-event systems using Petri nets," in *Applications and Theory of Petri Nets*, vol. 2679, Eindhoven, The Netherlands, June 2003, pp. 316–336.

[16] E. M. Clarke, O. Grumberg, and D. Peled, *Model checking*. MIT press, 1999.

[17] F. Basile, P. Chiacchio, and G. De Tommasi, "An efficient approach for online diagnosis of discrete event systems," *Automatic Control, IEEE Transactions on*, vol. 54, no. 4, pp. 748–759, 2009.

[18] K. Hiraishi and A. Ichikawa, "A class of petri nets that a necessary and sufficient condition for reachability is obtainable," *Trans. of SICE*, vol. 24, no. 6, pp. 635–640, 1988.